Secure operation guidelines

Getinge Connect Control Center and applications

1 About the guidelines

The secure operation guidelines describe how to securely operate Getinge Connect Control Center and its applications in a healthcare organization. The guidelines are intended for personnel responsible for information system security. This includes IT managers, IT security managers, and personnel that install and maintain Getinge Connect Control Center and its applications.

In these guidelines, Getinge Connect Control Center and its applications are referred to as *the system*.

1.1 Related documentation

The following documentation related to the system is available:

- Getinge Connect Control Center user's manual
- Getinge Connect Control Center installation instructions
- Servo TwinView user's manual

2 Secure operation guidelines

To ensure that the system operates securely, do as follows:

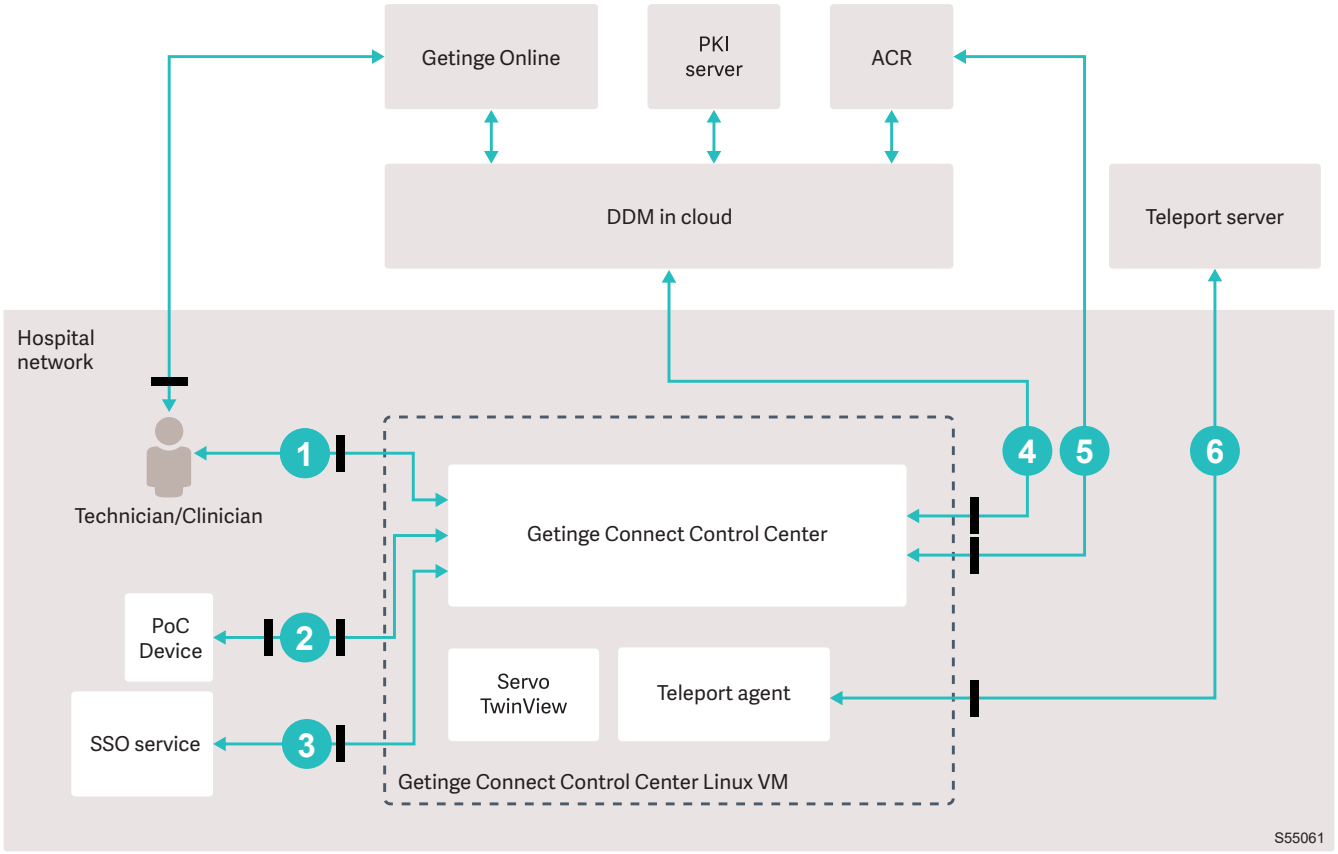
- Host the system on a dedicated physical server with restricted physical access control. Do not host other services on the same server.
- Make sure that hardware, firmware, and the operating system that the system is installed on is kept up to date.
- Harden the virtual machine that the system is installed on according to security configuration benchmarks. For example, according to the Center for Internet Security (CIS) or the Defence Information Systems Agency (DISA) benchmarks.
- Disable root access on the virtual machine that the system is installed on.
- Install software for intrusion detection and prevention on the virtual machine that the system is installed on.
- Monitor network traffic and host activity to detect and remediate malevolent activities.
- Make sure that devices and web browsers used to access the system are kept up to date and that their configuration is managed.

3 System overview

Getinge Connect Control Center runs on a local server set up by healthcare personnel. The server provides a runtime environment and common services for applications such as Servo TwinView. Point-of-care (PoC) devices connect and transfer data to Getinge Connect Control Center through the hospital network. The data is used by applications or Getinge Online.

Servo TwinView is a web-based application that subscribes to clinical and location data from Servo ventilator systems. The data is used to show twins of the user interfaces of connected ventilator systems in near real-time.

Getinge Online is a web-based service that supports device maintenance. In Getinge Online, PoC device logs and usage data is shown. Getinge Online also gives access to a public key infrastructure (PKI) server for certificate administration.



ID	Product interface	Network interface type	Internet layer	Transported or accessible assets (intrahospital unless indicated)
1	Web browser	Ethernet	WebSocket Secure/ HTTPS:443	Getinge Connect Control Center: Service and maintenance interface. Servo TwinView: Clinical and location data.
2	PoC device	Ethernet	MQTT/TLS:8883	PoC device onboarding, data transfer from PoC device, and over-the-air (OTA) software updates when applicable.
3	Single sign-on (SSO) service	Ethernet	HTTPS:9443	SSO integration to hospital Active Directory (AD).
4	Device and data manager (DDM) in cloud	Ethernet	HTTP/TLS:443	License token to establish MQTT connection.
			MQTT/TLS:443	PoC device onboarding, equipment data, and user account information.

ID	Product interface	Network interface type	Internet layer	Transported or accessible assets (intrahospital unless indicated)
5	Azure Container Registry (ACR)	Ethernet	HTTPS:443	Software installation or update. Application chart and images are pulled from the cloud registry.
6	Teleport	Ethernet	TLS:443	Remote assistance access to Getinge Connect Control Center from Getinge. Teleport connects to a Getinge server to enable remote access to Getinge Connect Control Center. Data transported is any data within Getinge Connect Control Center.

3.1 System environment

The system is intended to be used by healthcare providers in professional healthcare facilities. The system can be accessed anywhere on the healthcare organizations network.

Installation and use of the system outside of its intended system environment increases risk of physical and network based attacks.

Not following the intended system environment increases risk of:

- Downtime of the system and delayed information to applications. This is not considered to lead to increased risk of patient harm.
- Exposure of potentially sensitive information. See *5 Privacy risk profile* on page 4.

3.2 System requirements

It is recommended to use supported devices and web browsers to access the system. See supported devices and web browsers in the Getinge Connect Control Center user's manual and the Servo TwinView user's manual.

For requirements on the Getinge Connect Control Center server hardware, operating system, and network connection, see the Getinge Connect Control Center user's manual.

3.3 Security measures in the system

The following security measures are included in the system:

- All connections to the system are encrypted. See the figure and table in *3 System overview* on page 2.
- Connections to PoC devices and Getinge Online are authenticated through certificates. All certificates are signed through certificate signing requests (CSRs) to the Getinge PKI server.
- System security settings cannot be configured.
- Role based access to system functionality connects to the healthcare personnel AD through Security Assertion Markup Language (SAML) integration.
- Authenticity and integrity of software installations and updates are ensured through cryptographic signing of software packages.
- Remote assistance is done through a Teleport connection. No access to the system from Getinge is possible without local administrator activation of the connection.
- There is no failsafe mode for the system. Failsafe mode is N/A.

4 User roles and training

The following user roles are specified for the system:

- Technican role
- Clinican role

There are no special training requirements for users of the system.

5 Privacy risk profile

The system does not store collected data. Personally identifiable information, such as patient names and identification numbers, is not collected by the system.

Getinge Connect Control Center receives data from connected PoC devices. If installed, collected data can be sent to and shown in a web browser in Servo TwinView.

The system collects data about system use and treatment. This data can be seen as indirectly identifiable personal information because it is related to a device ID and timestamp. If set by the user, data can also be related to a location.

Getinge Connect Control Center sends equipment data to Getinge Online for maintenance and usage analysis. From Getinge Connect Control Center v1.2, it is possible to opt-out of data transfer to Getinge Online.

The healthcare organization must consider if the patient is to be informed about collection of information to fulfill the general data protection regulation (GDPR), the health insurance portability and accountability act (HIPAA), or similar national regulations on data privacy.

6 Recommended back-up policies

The system does not continuously store data that needs to be restored as part of a system recovery. However, to facilitate restoration of correct system function if there is a system failure, back-ups are recommended when changes are done in configuration and device location lists.

6.1 Incident action plan recommendations

If there is a suspected attack or if a severe vulnerability is discovered in the system it can be temporarily disabled without affecting the connected PoC devices clinical functionality.

If recommended by Getinge, Getinge Connect Control Center can be uninstalled and then installed again. See the Getinge Connect Control Center installation instructions.

7 Decommissioning

Before decommissioning Getinge Connect Control Center, keys and certificates stored in Kubernetes secrets must be erased.

Manufacturer:
Maquet Critical Care AB · Röntgenvägen 2 · 171 54 Solna · Sweden
www.getinge.com